VMware Cloud Foundation Architecture and Deployment Guide

14 JAN 2020

VMware Cloud Foundation 3.9

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About the VMware Cloud Foundation Architecture and Deployment Guide

The *VMware Cloud Foundation Architecture and Deployment Guide* provides a high-level overview of the VMware Cloud Foundation product and its architecture. This document also describes the deployment process for Cloud Foundation.

Intended Audience

The *VMware Cloud Foundation Architecture and Deployment Guide* is intended for data center cloud administrators who deploy a Cloud Foundation system in their organization's data center. The information in this guide is written for experienced data center cloud administrators who are familiar with:

- Concepts of virtualization and software-defined data centers
- Networking and concepts such as uplinks, NICs, and IP networks
- Hardware components such as top-of-rack (ToR) switches, inter-rack switches, servers with direct attached storage, cables, and power supplies
- Methods for setting up physical racks in your data center
- Using the VMware vSphere® Web Client™ to work with virtual machines

Related Publications

The *VMware Cloud Foundation Planning and Preparation Guide* provides detailed information about the software, tools, and external services that are required for Cloud Foundation.

The *VMware Cloud Foundation Operations and Administration Guide* contains detailed information about how to administer and operate a Cloud Foundation system in your data center.

Your Cloud Foundation system includes various VMware software products and components. You can find the documentation for those VMware software products at docs.vmware.com.

Cloud Foundation Glossary

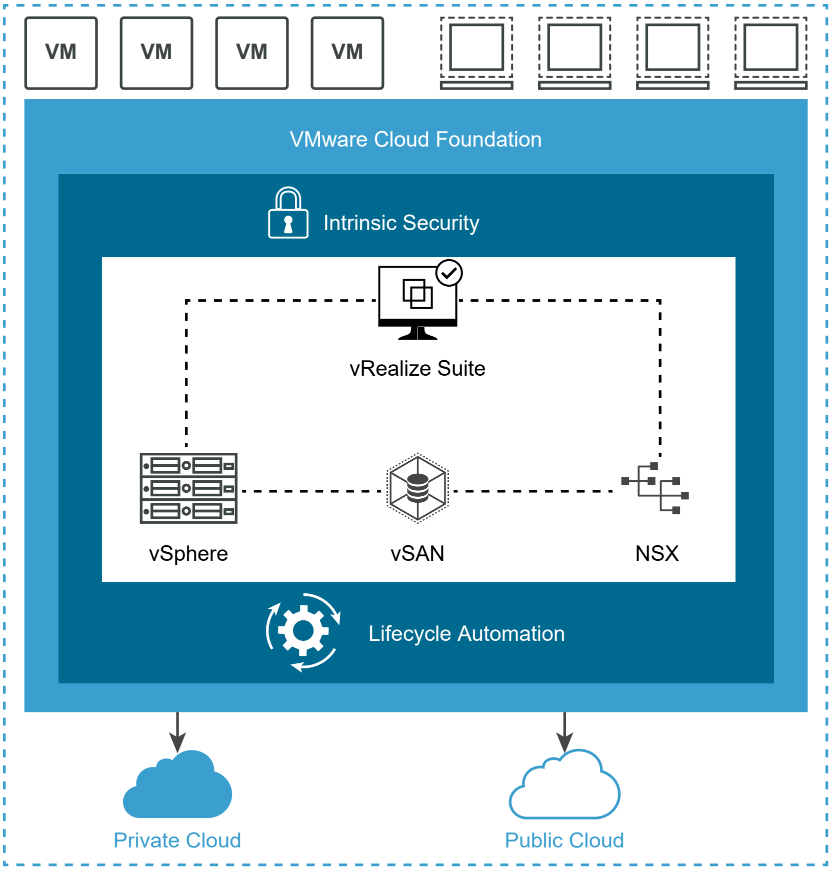
The Cloud Foundation Glossary defines terms specific to Cloud Foundation.

About VMware Cloud Foundation

1

VMware Cloud Foundation is an integrated software stack that bundles compute virtualization (VMware vSphere), storage virtualization (VMware vSAN), network virtualization (VMware NSX for vSphere and NSX-T), and cloud management (VMware vRealize Suite) into a single platform that can be deployed on premises as a private cloud or run as a service within a public cloud. You also have the option of using NFS or VMFS on FC storage for your workloads. Cloud Foundation helps to break down the traditional administrative silos in data centers, merging compute, storage, network provisioning, and cloud management to facilitate end-to-end support for application deployment.

This guide focuses on the private cloud use case.



Cloud Foundation uses VMware vCenter Server for virtual machine (VM) management, monitoring, and provisioning. Cloud Foundation also integrates with VMware vRealize Suite and supports other VMware products, including VMware Integrated OpenStack, VMware Integrated Containers, and VMware Horizon.

To manage the logical infrastructure in the private cloud, Cloud Foundation augments the VMware virtualization and management components with a new component, SDDC Manager. SDDC Manager automates the bring up, configuration, and provisioning of the entire SDDC stack. SDDC Manager also automates the lifecycle management of the stack. From this interface, the IT administrator can provision new private cloud resources, monitor changes to the logical infrastructure, and manage life cycle and other operational activities.

Cloud Foundation enables data center cloud administrators to provision an application environment in a rapid, repeatable, automated way versus the traditional manual process.

This chapter includes the following topics:

- Cloud Foundation Components
- Simplified Resource Provisioning with Workload Domains
- Automated Deployment of Horizon Components
- Automated Software Bring-Up
- Automated Lifecycle Management (LCM)
- Multi-Instance Management

Cloud Foundation Components

Cloud Foundation delivers a natively integrated software-defined data center stack that includes the core infrastructure virtualization, vSphere, vSAN and NSX.

SDDC Manager

SDDC Manager automates the entire system lifecycle (from initial bring-up, to configuration and provisioning, to upgrades and patching), and simplifies day-to-day management and operations.

VMware vSphere

VMware vSphere uses virtualization to transform individual data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. VMware vSphere manages these infrastructures as a unified operating environment and provides you with the tools to administer the data centers that participate in that environment.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.

VMware vSAN

VMware vSAN™ aggregates local or direct-attached data storage devices to create a single storage pool shared across all hosts in the vSAN cluster. vSAN eliminates the need for external shared storage, and simplifies storage configuration and virtual machine provisioning. Built in policies allow for flexibility in data availability.

NSX for vSphere and NSX-T

VI workload domains support the NSX for vSphere and NSX-T platforms.

NSX for vSphere provides networking and security functionality for your vSphere environment which allows networks and network services to be abstracted from the physical infrastructure. The ability to manage the network through software allows for rapid changes and increased security policies to be implemented.

NSX-T is focused on emerging application frameworks and architectures that have heterogeneous endpoints and technology stacks. NSX-T Data Center allows IT and development teams to choose the technologies best suited for their applications.

vRealize Suite

Cloud Foundation is integrated with the vRealize Suite of products.

vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager delivers complete lifecycle and content management capabilities for the VMware vRealize Suite. vRealize Suite Lifecycle Manager supports the deployment, upgrade, and patching of vRealize Log Insight, vRealize Automation, and vRealize Operations Manager.

vRealize Log Insight

Log Insight delivers heterogeneous and highly scalable log management with intuitive and actionable dashboards, sophisticated analytics, and broad third-party extensibility. It provides deep operational visibility and faster troubleshooting across physical, virtual and cloud environments.

Log Insight is installed by default for the management domain. You can add licenses to enable Log Insight for VI workload domains.

vRealize Automation

vRealize Automation is a cloud automation tool that accelerates the delivery of IT services through automation and pre-defined policies, providing high level of agility and flexibility for developers, while enabling IT teams to maintain frictionless governance and control. This is an optional component.

vRealize Operations Manager

vRealize Operations Manager delivers intelligent operations management with application-to-storage visibility across physical, virtual, and cloud infrastructures. Using policy-based automation, operations teams automate key processes and improve IT efficiency. This is an optional component.

Simplified Resource Provisioning with Workload Domains

Cloud Foundation introduces a new abstraction, workload domains, for creating logical pools across compute, storage, and networking. A workload domain consists of one or more vSphere clusters, provisioned automatically by SDDC Manager.

There are two types of workload domains - the management domain and VI workload domains.

The management domain is created during the bring-up process. It contains the Cloud Foundation management components. This includes an instance of vCenter Server and required NSX for vSphere components (NSX Manager and three NSX Controller VMs) for the management domain. All vRealize Suite components, such as vRealize Log Insight, vRealize Operations Manager, vRealize Automation, and vRealize Suite Lifecycle Manager, are installed in the management domain. The management domain uses vSAN storage.

Cloud Foundation implements Virtual Infrastructure (VI) workload domains for user workloads. You can choose the storage option (vSAN, NFS, or VMFS on FC) and NSX Platform (NSX for vSphere or NSX-T) for each VI workload domain. The workload domain can consist of one or more vSphere clusters. Each cluster starts with a minimum of three hosts and can scale up to the vSphere maximum of 64 hosts. SDDC Manager automates creation of the workload domain and the underlying vSphere cluster(s).

For each NSX for vSphere VI workload domain, SDDC Manager deploys an additional NSX Manager instance in the management domain to manage that VI workload domain. The three NSX Controller VMs are deployed in the VI workload domain cluster. These controller VMs communicate with the dedicated NSX Manager deployed in the management domain.

For the first NSX-T VI workload domain in your environment, SDDC Manager deploys a vCenter Server and NSX Manager cluster in the management domain. An additional vCenter Server is deployed for each subsequent NSX-T VI workload domain, but it shares the same NSX Manager cluster.

Automated Deployment of Horizon Components

A Horizon domain automates deployment of VMware Horizon components and supporting infrastructure to enable you to deliver Virtual Desktop Infrastructure (VDI) and Remote Desktop Session Host (RDSH) desktops and applications. These can be delivered as persistent, linked clone, or instant clone desktops. The Horizon domain can include VMware App Volumes for dynamic application mounting and User Environment Manager for a persistent end user experience.

Automated Software Bring-Up

You prepare your environment for Cloud Foundation by installing a baseline ESXi image on vSAN ReadyNodes. After the hosts are physically racked and cabled, Cloud Foundation uses the physical network details you provide (such as DNS, IP address pool, and so on) to automate the bring-up and configuration of the software stack. During bring-up, the management domain is created on the four hosts you specified. When the bring-up process completes, you have a functional management domain and can start provisioning VI workload domains.

Automated Lifecycle Management (LCM)

SDDC Manager automates upgrade and patch management for the SDDC software stack.

VMware provides update bundles for the SDDC stack, ensuring compatibility of all patches with installed components in your Cloud Foundation environment. You can apply an update to the management domain or VI workload domains independent of the other workload domains. This makes the process non-disruptive to tenant VMs.

Multi-Instance Management

Multiple Cloud Foundation instances can be managed together by grouping them into a federation, such that each member can view information about the entire federation and the individual instances within it. Federation members can view inventory across the Cloud Foundation instances in the federation as well as the available and used aggregate capacity (CPU, memory, and storage). This allows you to maintain control over the different sites and ensure that they are operating with the right degree of freedom and meeting compliance regulations for your industry. It also simplifies patch management by showing the number of patches available across sites in the global view.

Cloud Foundation Architecture

2

Cloud Foundation supports two architecture models - standard and consolidated.

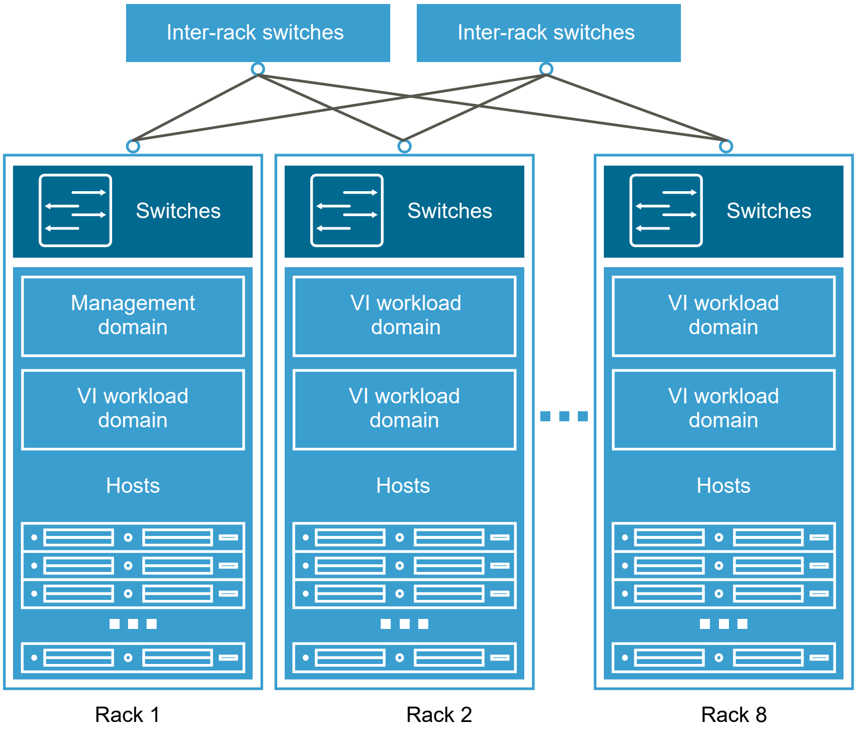
This chapter includes the following topics:

- Standard Architecture Model
- Consolidated Architecture Model

Standard Architecture Model

With the standard architecture model, management workloads run on a dedicated management domain and user workloads are deployed in separate virtual infrastructure (VI) workload domains. Each workload domain is managed by a separate vCenter Server instance which provides for scalability and allows for autonomous licensing and lifecycle management.

Figure 2-1. Sample Standard Architecture



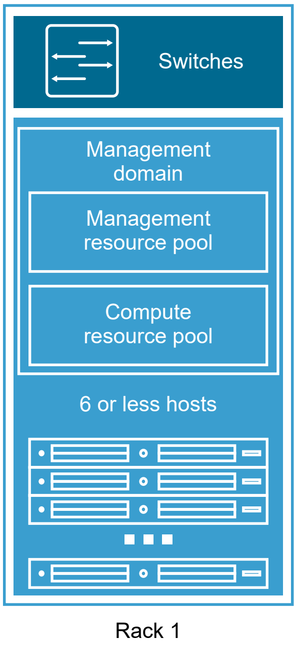
Standard architecture is the recommended model as it aligns with the VMware best practice of separating management workloads from customer workloads. It provides better long term flexibility and expansion options.

Consolidated Architecture Model

The consolidated architecture design targets smaller Cloud Foundation deployments and special use cases. In this design, the management and user workload domains run together on a shared management domain. The environment is managed from a single vCenter Server and vSphere resource pools provide isolation between management and user workloads. In a consolidated architecture model, care must be taken to ensure that resource pools are properly configured as the domain is shared by the management and compute workloads. The consolidated architecture does not support NSX-T or the automated deployment of Horizon and Enterprise PKS.

As you add additional hosts to a Cloud Foundation system deployed on a consolidated architecture, you can convert to the standard architecture by creating a VI workload domain and moving the user workload domain VMs from the compute resource pool to the newly created VI workload domain. After moving these VMs, you may need to update shares and reservations on the compute resource pool in the management domain.

Figure 2-2. Sample Consolidated Architecture



Preparing your Environment for Cloud Foundation

3

You must prepare your environment for deploying Cloud Foundation. See the *VMware Cloud Foundation Planning and Preparation Guide*.

Deploying Cloud Foundation

4

You begin the Cloud Foundation deployment process by deploying the Cloud Builder VM. The Cloud Builder VM includes the VMware Imaging Appliance, which you use to image your servers with ESXi software. After imaging your servers, you download and complete the deployment parameters sheet from the Cloud Builder VM to define your network information, host details, and other required information. During the deployment process, this spreadsheet is automatically then converted to a JSON file and uploaded to the Cloud Builder VM. The provided information is validated, and the automated phase of the deployment process begins.

Prerequisites

You must prepare your environment for deploying Cloud Foundation. See the *VMware Cloud Foundation Planning and Preparation Guide*.

Procedure

1 Deploy Cloud Builder VM

   The Cloud Foundation Builder VM is a VM which includes the VMware Imaging Appliance for installing ESXi on your servers. After you image the servers, use the Cloud Builder VM to deploy and configure the management domain and transfer inventory and control to SDDC Manager. During the deployment process, the Cloud Foundation Builder VM validates network information you provide in the deployment parameter spreadsheet such as DNS, network (VLANS, IPs, MTUs), and credentials.

2 Installing ESXi Software on Cloud Foundation Servers

   You can use the VMware Imaging Appliance (VIA) included with the Cloud Builder VM to image servers for use in the management domain and VI workload domains.

3 Initiate the Cloud Foundation Bring-Up Process

   The Cloud Foundation deployment process is referred to as bring-up. You specify deployment information specific to your environment such as networks, hosts, license keys, and other information in the deployment parameter spreadsheet and upload the file. During bring-up, the management domain is created on the ESXi hosts specified in the deployment configuration spreadsheet. The Cloud Foundation software components are automatically deployed, configured, and licensed using the information provided.

4 Configure Dual Authentication

You must configure dual authentication in order to perform certain tasks, such as updating or rotating passwords and configuring NSX Manager backups.

Deploy Cloud Builder VM

The Cloud Foundation Builder VM is a VM which includes the VMware Imaging Appliance for installing ESXi on your servers. After you image the servers, use the Cloud Builder VM to deploy and configure the management domain and transfer inventory and control to SDDC Manager. During the deployment process, the Cloud Foundation Builder VM validates network information you provide in the deployment parameter spreadsheet such as DNS, network (VLANS, IPs, MTUs), and credentials.

You must deploy the Cloud Builder VM on a suitable platform. This can be on a laptop under VMware Workstation or VMware Fusion, or on an ESXi host. The Cloud Builder VM must have network access to all hosts on the management network. Approximately 11 to 350 gigabytes of storage is required to deploy the Cloud Builder VM.

The procedure here describes deploying the Cloud Builder VM on an ESXi host. Other deployment methods have different procedures.

Prerequisites

To image servers and automate the deployment, the Cloud Builder VM must be on the same management network as the hosts to be used. It must also be able to access all required external services, such as DNS and NTP.

Procedure

1. Download the Cloud Builder VM OVA on the Windows machine.
2. Log in to the vSphere Host Client.
3. In the navigator, select **Host**.
4. Click **Create/Register VM**.
5. On the Select creation type dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
6. Enter a name for the VM.
7. Select **Click to select files or drag/drop**. Select the Cloud Builder VM OVA from your local file system and click **Open**.
8. Click **Next**.
9. On the Select Storage page, select the storage for the Cloud Builder VM.
10. On the License agreements dialog box, click **I agree** and then click **Next**.
11. On the Select networks dialog box, select the port group associated with the VLAN ID used by the ESXi hosts where Cloud Foundation will be deployed and then click **Next**.

12 On the Additional settings dialog box, expand **Application** and enter the following information for the Cloud Builder VM:

Setting	Details
Deployment Architecture	Do not change the default (**vcf**) value.
Admin Username	The admin user name cannot be one of the following pre-defined user names: ■ root ■ bin ■ daemon ■ messagebus ■ systemd-bus-proxy ■ systemd-journal-gateway ■ systemd-journal-remote ■ systemd-journal-upload ■ systemd-network ■ systemd-resolve ■ systemd-timesync ■ nobody ■ sshd ■ named ■ rpc ■ tftp ■ ntp ■ smmsp ■ cassandra
Admin Password/Admin Password confirm	The admin password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.
Root password/Root password confirm	The root password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.
Hostname	Enter the hostname for the Cloud Builder VM.
Network 1 IP Address	Enter the IP address for the Cloud Builder VM.
Network 1 Subnet Mask	For example, `255.255.255.0`.
Default Gateway	Enter the default gateway for the Cloud Builder VM.
DNS Servers	IP address of the primary and secondary DNS servers (comma separated). Do not specify more than two servers.
DNS Domain Name	For example, `vsphere.local`.
DNS Domain Search Paths	Comma separated. For example `vsphere.local, sf.vsphere.local`.
NTP Servers	Comma separated.

13 Review the deployment details and click **Finish**.

> **Note** Make sure your passwords meet the requirements specified above before clicking **Finish** or your deployment will not succeed.

14 After the Cloud Builder VM is deployed, SSH in to the VM with the admin credentials provided in step 12.

15 Ensure that you can ping the ESXi hosts.

16 Verify that the Cloud Builder VM has access to the required external services, such as DNS and NTP by performing forward and reverse DNS lookups for each host and the specified NTP servers.

Installing ESXi Software on Cloud Foundation Servers

You can use the VMware Imaging Appliance (VIA) included with the Cloud Builder VM to image servers for use in the management domain and VI workload domains.

Before you can complete the deployment parameters spreadsheet to define your network information, host details, and other required information, you must install ESXi on your servers. If your servers are already installed with a supported version of ESXi, you can skip imaging. Otherwise, you can use VIA.

This guide describes using VIA to image servers prior to bring-up of a Cloud Foundation system. You can also use VIA to image servers prior to adding them to Cloud Foundation as part of the host commissioning process after bring-up is complete. See the *VMware Cloud Foundation Operations and Administration Guide* for more information.

Server Prerequisites

The servers that you image must meet certain prerequisites:

- PXE Boot is configured as primary boot option
- Install device is configured as the second boot option
- Legacy boot mode configured in BIOS (UEFI boot mode is not supported)
- Servers are in the same L2 domain as the Cloud Builder VM
- Servers are reachable over an untagged VLAN/Network (VLAN ID 0)
- The Cloud Builder VM is deployed on an untagged VLAN/Network
- Server hardware/firmware should be configured for virtualization and vSAN and match the Cloud Foundation BOM as described in the Release Notes
- Physical hardware health status should be "healthy" without any errors
- Any onboard NICs are disabled on the servers and only the two 10 GbE NICs reserved for use with Cloud Foundation are enabled in BIOS

The default root credentials for servers imaged with VIA are user `root`, password `EvoSddc!2016`.

Download ESXi Software and VIBs

In order to image your servers, you need to download an ESXi ISO and any vSphere Installation Bundles (VIBs) required to get the servers to a supported version of ESXi. See the BOM section of the VMware Cloud Foundation Release Notes for information about ESXi support.

You can download the ISO and VIBs from My VMware (https://my.vmware.com) to any location on the Windows machine that is connected to the Cloud Builder VM. Make sure to record the MD5 or SHA-1 checksums. You will need them when you upload the ISO/VIB to the VMware Imaging Appliance.

Provide Network Information for Imaging

You must provide the VMware Imaging Appliance with certain network information specific to your environment before you can image your servers. This information is contained in the `via.properties` file on the Cloud Builder VM.

Procedure

1. SSH into the Cloud Builder VM using the credentials specified when you deployed the VM. See Deploy Cloud Builder VM.
2. Type `su` to switch to the root user.
3. Navigate to the `/opt/vmware/evorack-imaging/config/` directory.

4 Update the `via.properties` file with your network information.

   a If the Cloud Builder VM is using the `eth0` interface (default), then you do not need to modify any of the properties in Section A. If the Cloud Builder VM has multiple network interfaces and is not using `eth0`, you must update the following properties.

Property	Description
via.network.interface	Interface of the Cloud Builder VM configured in management network.
via.web.url	The IP address used to access the VMware Imaging Appliance UI. Update this with the IP address of Cloud Builder VM in the management network.
via.network.ifaceaddr	Update this with the IP address of Cloud Builder VM in the management network.
via.dhcp.esxi.tftpServer	IP address of the server where TFTP is running. Update this with the IP address of Cloud Builder VM in the management network.
via.config.remote.pxe=false	Do not modify.

   b Update Section B with the network information for your environment.

Property	Description
via.dhcp.netmask	Netmask of the management network.
via.dhcp.subnet	Subnet of the management network.
via.dhcp.routers	Gateway IP of the management network.
via.esxi.firewall.allowed.network	CIDR notation for subnet IP of the management network.

5 Type **`systemctl restart imaging.service`** to restart the imaging service.

   Wait for the imaging service to restart.

6 Type **`systemctl status imaging.service`** to verify that the imaging service is running.

What to do next

Log in to the VMware Imaging Appliance and upload software.

Upload ISOs and VIBs to the VMware Imaging Appliance

After you have downloaded the required software and updated `via.properties` with your network information, you can upload ISOs and VIBs to the VMware Imaging Appliance.

Procedure

1 In a web browser on the Windows machine that is connected to the Cloud Builder VM, navigate to `https://`*`Cloud_Builder_VM_IP`*`:8445/via`.

   The VMware Imaging Appliance page displays.

2 Enter the admin credentials you provided when you deployed the Cloud Builder VM and click Log in.

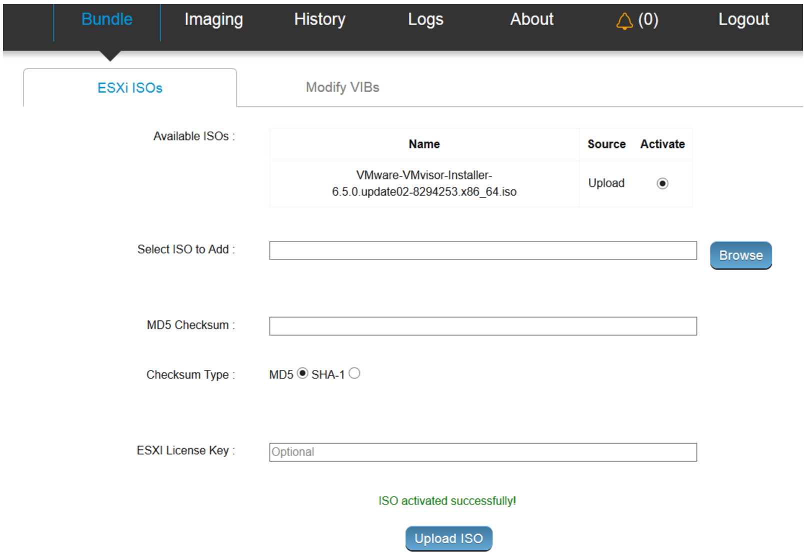
3 Click **Bundle** and then click the **ESXi ISOs** tab.

4 Click **Browse** to locate and select the ISO.

5 Select the checksum type and enter the checksum.

6 Click **Upload ISO**.

7 When the uploaded ISO appears, select **Activate** to use the ISO for imaging servers.



Available ISOs :

Name	Source	Activate
VMware-VMvisor-Installer-6.5.0.update02-8294253.x86_64.iso	Upload	●

Select ISO to Add :

MD5 Checksum :

Checksum Type : MD5 ● SHA-1 ○

ESXi License Key : Optional

ISO activated successfully!

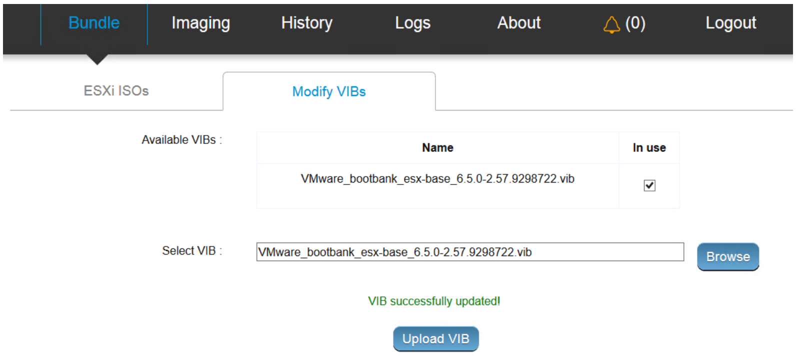
8 Click the **Modify VIBs** tab.

The steps for uploading VIBs are optional.

9 Click **Browse** to locate and select the VIB.

10 Click **Upload VIB**.

11 When the uploaded VIB appears, select **In use** to use the VIB for imaging servers.



Available VIBs :

Name	In use
VMware_bootbank_esx-base_6.5.0-2.57.9298722.vib	☑

Select VIB : VMware_bootbank_esx-base_6.5.0-2.57.9298722.vib

VIB successfully updated!

What to do next

Use the selected ISO and VIB(s) to image servers for use with Cloud Foundation.

Image Servers with ESXi and VIBs

Once you have uploaded the required ESXi and VIB packages to the VMware Imaging Appliance, you can begin imaging servers. You can image an individual server, or multiple servers at the same time.

You can use VIA to image servers for use in the management domain and VI workload domains. The management domain requires a minimum of four servers. See the *VMware Cloud Foundation Planning and Preparation Guide* for more information about requirements.

Note When you image servers, VIA uses the ESXi ISO that you activated and the VIB(s) that you marked as **In use**.

Procedure

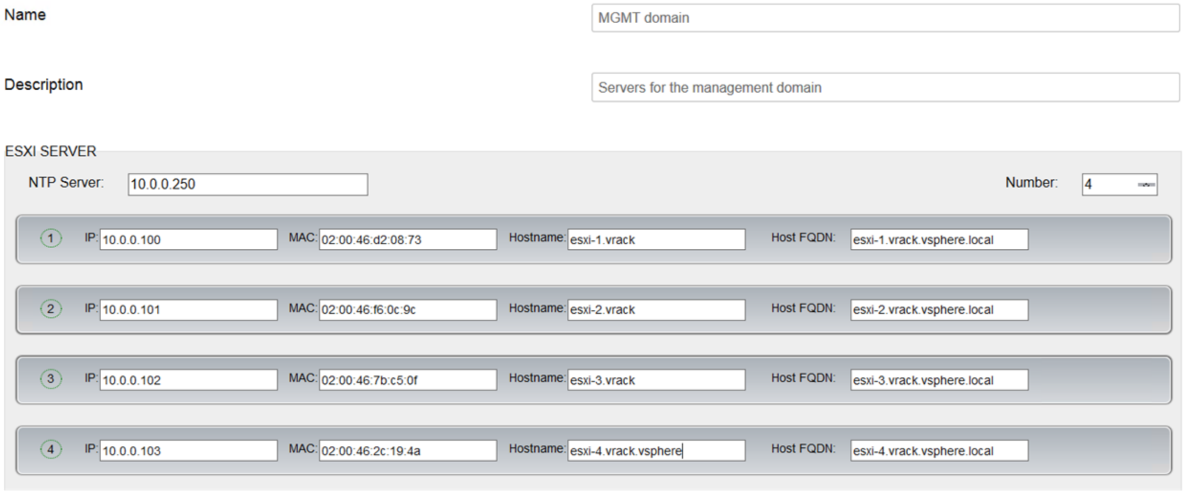
1 In a web browser on the Windows machine that is connected to the Cloud Builder VM, navigate to `https://`*`Cloud_Builder_VM_IP`*`:8445/via`.

The VMware Imaging Appliance page displays.

2 Enter the admin credentials you provided when you deployed the Cloud Builder VM and click Log in.

3 Click Imaging.

4 Enter the required information.



Name: MGMT domain

Description: Servers for the management domain

ESXI SERVER

NTP Server: 10.0.0.250

Number: 4

1 IP: 10.0.0.100 MAC: 02:00:46:d2:08:73 Hostname: esxi-1.vrack Host FQDN: esxi-1.vrack.vsphere.local

2 IP: 10.0.0.101 MAC: 02:00:46:f6:0c:9c Hostname: esxi-2.vrack Host FQDN: esxi-2.vrack.vsphere.local

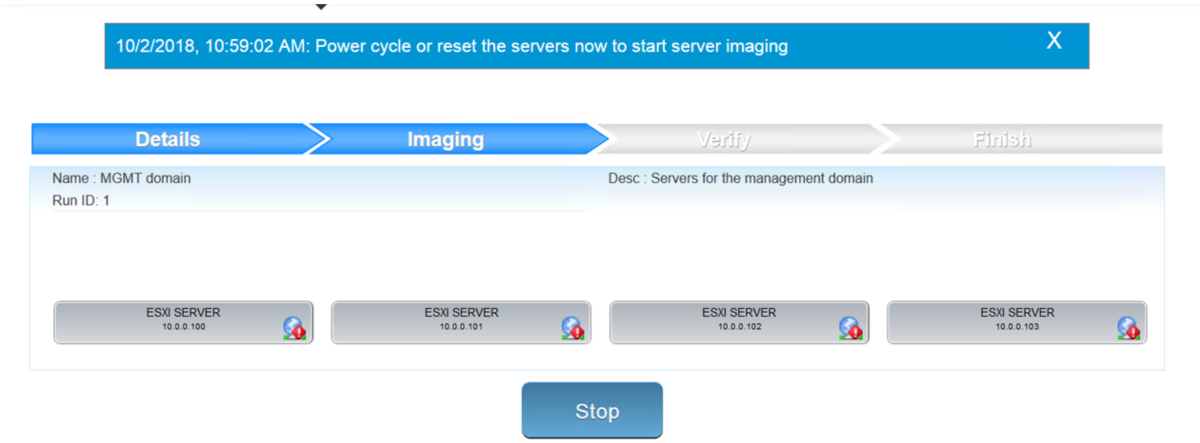
3 IP: 10.0.0.102 MAC: 02:00:46:7b:c5:0f Hostname: esxi-3.vrack Host FQDN: esxi-3.vrack.vsphere.local

4 IP: 10.0.0.103 MAC: 02:00:46:2c:19:4a Hostname: esxi-4.vrack.vsphere Host FQDN: esxi-4.vrack.vsphere.local

Option	Description
Name	Enter a name for the imaging job.
Number	Enter the number of servers you want to image with the selected ISO and VIBs.
Description	Enter a description for the imaging job.
NTP Server	Enter the IP address for the NTP server.
IP	Enter the IP address for the server.
MAC	Enter the MAC address for the server.
Hostname	Enter the hostname for the server.
Host FQDN	Enter the FQDN for the server.

5 Click **Start Imaging**.

6 When prompted, power cycle the server(s) to continue imaging.



10/2/2018, 10:59:02 AM: Power cycle or reset the servers now to start server imaging

Name : MGMT domain

Run ID: 1

Desc : Servers for the management domain

VIA displays information about the progress of imaging. Click a server to view details. Once imaging is complete, VIA performs verification of the servers.

7 When verification is finished, click **Complete**.

What to do next

Perform post-imaging tasks before you download the deployment parameter sheet and begin the bring-up process.

Post-Imaging Tasks

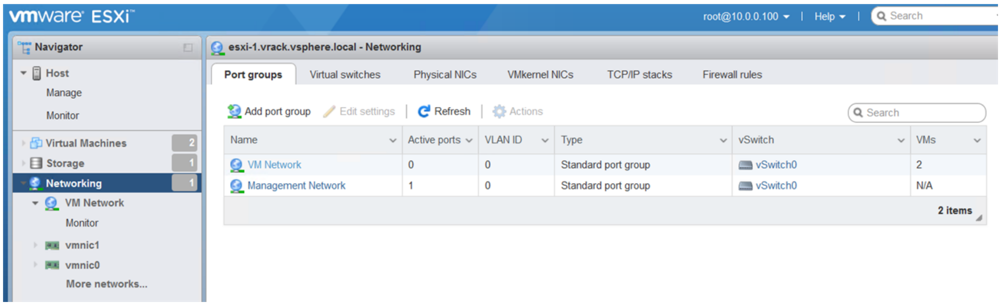
After you image your servers with ESXi and VIBs, you must perform some post-imaging tasks, depending on whether you use an untagged or a tagged management VLAN.

For imaging servers, the VMware Imaging Appliance requires an untagged VLAN. You can continue to use an untagged VLAN for management, or you can use a tagged VLAN.

Untagged Management VLAN

In this scenario, you use the same network for provisioning and management.

- Ensure that the Management Network and VM Network port groups on each host use the untagged VLAN (VLAN ID 0)



esxi-1.vrack.vsphere.local - Networking

Name	Active ports	VLAN ID	Type	vSwitch	VMs
VM Network	0	0	Standard port group	vSwitch0	2
Management Network	1	0	Standard port group	vSwitch0	N/A

2 items

- Verify that your DNS and NTP server are routable to the management network and ESXi hosts can reach them. To configure a default gateway or static routes on your ESXi hosts, see https://kb.vmware.com/kb/2001426.

Tagged Management VLAN

In this scenario, you use an untagged VLAN for provisioning and a tagged VLAN for management.

- Modify the Management Network and VM Network port groups on each host to use the tagged VLAN
- Migrate the hosts from the provisioning network to the management network on the TOR switches
- Verify that your DNS and NTP server are routable to the management network and ESXi hosts can reach them. To configure a default gateway or static routes on your ESXi hosts, see https://kb.vmware.com/kb/2001426.

Initiate the Cloud Foundation Bring-Up Process

The Cloud Foundation deployment process is referred to as bring-up. You specify deployment information specific to your environment such as networks, hosts, license keys, and other information in the deployment parameter spreadsheet and upload the file. During bring-up, the management domain is created on the ESXi hosts specified in the deployment configuration spreadsheet. The Cloud Foundation software components are automatically deployed, configured, and licensed using the information provided.

Download and Complete Deployment Parameter Sheet

The deployment parameter spreadsheet provides a mechanism to specify infrastructure information specific to your environment. This includes information about your networks, hosts, license keys, and other information. The spreadsheet is downloaded from the Cloud Builder VM and the completed spreadsheet is uploaded back to the VM. The deployment parameter spreadsheet can be reused to deploy multiple Cloud Foundation instances of the same version.

Cloud Foundation 3.9.1 supports isolating VMkernel traffic (management, vSAN, vMotion, or overlay) across multiple physical NICs (pNICs). However, you cannot use the deployment parameter sheet for bring-up of hosts with more than two pNICs. To perform bring-up with hosts with more than two pNICs, use the VMware Cloud Foundation API.

Procedure

1. In a web browser on the Windows machine that is connected to the Cloud Builder VM, navigate to `https://`*`Cloud_Builder_VM_IP`*.

   For Cloud Foundation 3.9, the VMware Cloud Foundation login page appears. For Cloud Foundation 3.9.1, the Welcome to VMware Cloud Builder login page appears.

2. Enter the admin credentials you provided when you deployed the Cloud Builder VM and then click **Log In**.

3. Read the End-User License Agreement and accept it. Click **Next**.

4. If you are deploying Cloud Foundation 3.9.1, select **VMware Cloud Foundation** on the Supported Platform page and click **Next**.

   Ignore this step if you are deploying Cloud Foundation 3.9.

5 Review the prerequisites checklist and ensure the requirements are met before proceeding. If there are any gaps, ensure they are fixed before proceeding to avoid issues during the the bring-up process.

   For Cloud Foundation 3.9, select the checkbox for each prerequisite or select the Check All checkbox.

   For Cloud Foundation 3.9.1, select the checkbox at the bottom of the page to acknowlege that your environment meets the listed requirements. You can download or print the prerequisite list as well.

6 Click **Next**.

7 In the Download Spreadsheet section, click **Download**.

8 Complete the spreadsheet. See About the Deployment Parameter Sheet.

About the Deployment Parameter Sheet

The deployment parameter Excel sheet contains tabs categorizing the information required for deploying Cloud Foundation. The information provided is used to create the management domain.

The fields in yellow contain sample values that you can overwrite as appropriate. If a cell turns red, the required information is missing, or validation has failed. All other information (including default values) are for your reference only. Modifying any of these fields can lead to deployment errors.

Prerequisites Checklist Tab

This tab is a summary of infrastructure configuration requirements that need to be satisfied before deploying Cloud Foundation.

The VMware Cloud Builder runs a platform audit before starting deployment to check if the requirements listed on this tab are met. If the audit fails, you cannot proceed with the deployment.

Physical Hardware

Servers must be racked and cabled. ESXi version as mentioned in the *VMware Cloud Foundation Release Notes* must be installed on each host.

For additional details on hardware requirements, see the *VMware Cloud Foundation Planning and Preparation Guide*.

ESXi Configuration

All ESXi hosts must be configured with the following settings:

- Static IP address assigned to the management interface (vmk0)
- Management network portgroup configured with correct VLAN ID
- VM network portgroup configured with the same VLAN ID as the management network
- TSM-SSH service enabled and policy set to `Start and Stop with Host`
- NTP service enabled, configured, and policy set to `Start and Stop with Host`

If you used the VMware Imaging Appliance to install ESXi on your hosts and you completed the Post-Imaging Tasks, then your hosts are already configured properly and are ready for bring-up.

Management Workloads Tab

This tab provides an overview of the components deployed by the Cloud Builder VM. The sizes and versions are not editable and are provided for reference only.

Input required:

- In column L, update the six red fields with your license keys. Ensure the license key matches the product and version listed in each row. The license key audit during bring-up only validates the format of the key, not the accuracy of the key.

  The required license keys are:

  - ESXi
  - vSAN
  - vCenter Server
  - NSX for vSphere
  - SDDC Manager
  - vRealize Log Insight

If you do not enter license keys for these products, you will not be able to create or expand VI workload domains.

Users and Groups Tab

This tab details the accounts and initial passwords for the Cloud Foundation components. You must provide input for each yellow box. A red cell may indicate that validations on the password length has failed.

Input Required

Update the Default Password field for each user (including the automation user in the last row). Passwords can be different per user or common across multiple users. The tables below provide details on password requirements.

Table 4-1. Password Complexity

Password	Complexity
ESXi Hosts	This is the password which you configured on the hosts during ESXi installation.
Default Single-Sign on Domain User	SSO
vCenter Server and Platform Services Controller virtual appliance root account	SSO
NSX Manager Administrator account	Standard
NSX Manager CLI	Standard
NSX Controller Admin	Standard
Operations Management Layer	
vRealize Log Insight admin account	vRLI

Table 4-1. Password Complexity (continued)

Password	Complexity
vRealize Log Insight root account	Standard
SDDC Manager	
SDDC Manager appliance root account	Standard
SDDC Manager super user	Standard
SDDC Manager REST API user	Standard

Table 4-2. Password Requirements based on Complexity

Password Type	Requirements Based on Complexity
Standard	1 Length 8-12 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character such as @ ! # $ % ^ or ? 3 Cannot include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
SSO (accounts in SSO vsphere.local)	1 Length 8-20 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character
vRLI	1 Length 8-12 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character 3 Must not include a character repeated more than twice

Hosts and Networks tab

In this tab, specify details of your existing networking infrastructure. This information is configured on the appropriate Cloud Foundation components.

Management Cluster

This section covers the VLANs, gateways, MTU, and expected IP ranges and subnet mask for each network you have configured on the Top of Rack switches in your environment.

Table 4-3. Input Required

VLAN	Portgroup Name - Do not modify	CIDR Notation	Gateway	MTU
Enter VLAN ID for management network. The VLAN ID can be between 0 and 4094. **Note** Enter 0 if you imaged the servers with VIA. VLAN 0 means the management network is untagged.	SDDC-DPortGroup-Mgmt	Enter CIDR notation for management network	Enter gateway IP for management network	Enter MTU for management network. The MTU can be between 1500 and 9000.
Enter VLAN ID for vMotion network The VLAN ID can be between 0 and 4094.	SDDC-DPortGroup-vMotion	Enter CIDR notation for vMotion network	Enter gateway IP for vMotion network	Enter MTU for vMotion network The MTU can be between 1500 and 9000.
Enter VLAN ID for vSAN network The VLAN ID can be between 0 and 4094.	SDDC-DPortGroup-VSAN	Enter CIDR notation for vSAN network	Enter gateway IP for vSAN network	Enter MTU for vSAN network The MTU can be between 1500 and 9000.
Enter VLAN ID for VXLAN network The VLAN ID can be between 0 and 4094.	VXLAN (VTEP) - DHCP Network	n/a Cloud Foundation uses DHCP for VTEPs, so VXLAN CIDR is not required.	n/a Cloud Foundation uses DHCP for VTEPs, so VXLAN gateway is not required.	Enter MTU for VXLAN network The MTU can be between 1500 and 9000.
Enter VLAN ID for the first uplink. The VLAN ID can be between 0 and 4094.	sfo01-m010mgmt01-uplink01	Enter CIDR notation for the first uplink	Enter gateway IP for the first uplink	Enter MTU for the first uplink The MTU can be between 1500 and 9000.
Enter VLAN ID for the second uplink. The VLAN ID can be between 0 and 4094.	sfo01-m010mgmt01-uplink02	Enter CIDR notation for the second uplink	Enter gateway IP for the second uplink	Enter MTU for the second uplink The MTU can be between 1500 and 9000.

Management Hosts

Specify the IP addresses of the ESXi hosts where the management domain is to be configured. In a standard deployment, only four hosts are required in the management domain. Cloud Foundation can also be deployed in a consolidated method. In the consolidated deployment method, all workloads are deployed in the management domain instead of a separate workload domain. As such, additional hosts may be required to provide the capacity needed. In this section, only enter values for the number of hosts desired in the management domain.

Table 4-4. Input Required

Host Name	IP Address
sfo01m01esx01	Enter IP address of first ESXi host where Cloud Foundation is to be deployed.
sfo01m01esx02	Enter IP address of second ESXi host

Table 4-4. Input Required (continued)

Host Name	IP Address
sfo01m01esx03	Enter IP address of third ESXi host
sfo01m01esx04	Enter IP address of fourth ESXi host

Inclusion Ranges

Specify IP inclusion ranges for the vSAN and vMotion networks of the management domain. IP addresses from the specified range are automatically assigned to hosts. Ensure that the IP ranges include sufficient IP addresses for the initial deployment. The number of IP addresses must be at least equal to the number of hosts deployed as part of Cloud Foundation.

As an example, if you specify the range start value as 192.168.1.1 and end as 192.168.1.20, a total of 20 IP addresses would be used.

Do not use special IP addresses, such as the network or broadcast address.

IPs for the vMotion range must be part of the VLAN configured with the SDDC-Dswitch-Private-vmotion. IPs for the vSAN range must be part of the VLAN configured for the SDDC-Dswitch-Private-vsan. All IPs within the range must be available for use or IP conflicts will occur. It is a good practice to validate this prior to starting a deployment.

Table 4-5. Input Required

Portgrpup Name - Do not modify	Start	End
SDDC-DPortGroup-vMotion	Enter start of IP address range for vMotion network.	Enter end of IP address range.
SDDC-DPortGroup-VSAN	Enter start of IP address range for vMotion network.	Enter end of IP address range.

ESXi Host Security Thumbprints

If you want bring-up to validate the SSH fingerprint and SSL thumbprints of the hosts before connecting to them, select **Yes** in the **Validate ESXi Thumbprints** field.

If you set **Validate ESXi Thumbprints** to **Yes**, follow the steps below.

1 Open the DCUI screen for each server.

2 From the View Support Information tab, copy the SSH RSA Key Fingerprint and SSL Thumbprint.

3 Replace the example values in the parameter sheet with these values.

Deploy Parameters Tab: Existing Infrastructure Details

Your existing DNS infrastructure is used to provide forward and reverse name resolution for all hosts and VMs in the Cloud Foundation SDDC. External NTP sources are also utilized to synchronize the time between the software components.

Table 4-6. Infrastructure

Parameter	Value
DNS Server #1	Enter IP address of first DNS server.
DNS Server #2	Enter IP address of second DNS server. If you have only one DNS server, enter n/a in this cell.
NTP Server #1	Enter IP address or FQDN of first NTP server.
NTP Server #2	Enter IP address or FQDN of second NTP server. If you have only one NTP server, enter n/a in this cell.

Table 4-7. Single-Sign-On Site Name

Parameter	Value
Single-sign-on Site Name	Enter an abbreviation for the physical region where this installation is based. The site name is used by the Platform Service Controller.

Table 4-8. DNS Zone

Parameter	Value
DNS Zone Name	Enter root domain name for your SDDC management components.

Table 4-9. Datastores

Parameter	Value
vSAN Datastore Name	Enter vSAN datastore name for your management components.
Enable vSAN Deduplication and Compression	Select Yes to turn on Dedupe and Compression capabilities of vSAN.

Table 4-10. CEIP

Parameter	Value
Enable Customer Experience Improvement Program (“CEIP”)	Select an option to enable or disable CEIP across vSphere, NSX, vSAN and vRLI during Cloud Builder deployment.

Deploy Parameters Tab: vSphere Infrastructure

Specify host names and IP addresses for the vCenter and Platform Service Controllers.

This section of the deployment parameter sheet contains sample host names, but you can update them with names that meet your naming standards. This host name is one part of the FQDN - the second part of the FQDN is the root or child DNS zone name provided above.

The specified host names and IP addresses must be resolvable using the DNS servers provided earlier, both forward (hostname to IP) and reverse (IP to hostname), otherwise the bring-up process will fail.

Table 4-11. Management Cluster

Parameter	Host Name	IP Address
vCenter Server	Enter a host name for the vCenter Server.	Enter the IP address for the vCenter Server that is part of the management VLAN. This is the same VLAN and IP address space where the vCenter, PSC, and ESXi management VMKernels reside.
Platform Service Controller	Enter a host name for the Platform Service Controller.	Enter the IP address for the Platform Service Controller that is part of the management VLAN. This is the same VLAN and IP address space where the vCenter, PSC, and ESXi management VMKernels reside.
Second Platform Service Controller	Enter a host name for the second Platform Service Controller.	Enter the IP address for the Platform Service Controller that is part of the management VLAN. This is the same VLAN and IP address space where the vCenter, PSC, and ESXi management VMKernels reside.
vCenter Server Appliance Size (Default Small)	This parameter defines the size of the vCenter Server to be deployed. Default size is Small. Additional options are: tiny, medium, large, and xlarge.	

Table 4-12. vCenter Objects

Parameter	Value
Datacenter Name - Management	Enter a name for the management datacenter. Also enter the Enhanced vMotion value set on the host cluster. To enable EVC on the management cluster, select the CPU chipset that should be applied to enhance vMotion compatability.
Cluster Name - Management	Enter a name for the management cluster.
vSphere Distributed Switch Name	Enter a name for the management vSphere distributed name.
vSphere Distributed Switch MTU Size	Enter the MTU size. Default value is 9000.
Default vSS Portgroup Name	Do not change the default value `VM Network`.

Table 4-13. vCenter Resource Pools

Parameter	Value
Resource Pool SDDC Mgmt	Specify the vCenter resource pool name for management VMs.
Resource Pool SDDC Edge	Specify the vCenter resource pool name for NSX VMs.
Resource Pool User Edge	Specify the vCenter resource pool name for user deployed NSX VMs in a consolidated architecture.
Resource Pool User VM	Specify the vCenter resource pool name for user deployed workload VMs in a consolidated architecture.

In the Virtual Networking - ESXi Hosts section below, the default settings are appropriate for hosts with two physical NICs (pNICs). To perform bring-up with hosts with more than two pNICs, use the VMware Cloud Foundation API.

Table 4-14. Virtual Networking - ESXi Hosts

Parameter	Value
Physical NIC to Assign to vDS - Management	Select the physical NIC to assign to the management vDS.
VMKernel Adaptor for Management	Select the vmkernel adaptor to assign to the management network.
vSphere Standard Switch - Management	Do not modify.
vmnic Allocated to vSS - Management	Select the physical NIC to assign to the management vSS.

Table 4-15. Region A Configuration Details

Parameter	Value
Join Existing Single-Sign-On Domain	■ Select No if you are deploying the first Cloud Foundation instance. ■ Select Yes if you are deploying the second Cloud Foundation instance. Then complete the remaining values in this section.
Platform Service Controller IP Address	Enter the IP address of the Platform Service Controller of the first instance.
Platform Service Controller SSO Username	Enter the user name for the Platform Service Controller of the first instance.
Platform Service Controller SSO Password	Enter the password for the Platform Service Controller of the first instance.

Deploy Parameters Tab: NSX

Enter IP addresses and host names for NSX installation.

The requirements vary depending on your version of Cloud Foundation. The following tables indicate any version-specific requirements.

Table 4-16. Management Cluster

Parameter	Value
NSX Manager	Enter the host name and IP address for the NSX Manager. The host name can match your naming standards but must be registered in DNS with both forward and reverse resolution matching the specified IP. The IP address must be part of the management VLAN. This is the same VLAN and IP address space where the vCenter, PSC, and ESXi management VMKernels reside.
NSX Controller IP Pool Start Address	In IP Address, enter the starting IP address of the IP address range. Each IP in the range, including the starting and ending IP address, must be unused in your environment.
NSX Controller IP Pool End Address	In IP Address, enter the end IP address of the IP address range. Each IP in the range, including the starting and ending IP address, must be unused in your environment.

Table 4-17. Management Domain - Segment IDs

Parameter	Value
NSX Segment ID Range	Default values for the segment ID range. The segment ID range is used for NSX virtual wires. These are not exposed outside of the NSX environment. Only modify these values if the default range is being used in another NSX deployment within your environment.
NSX Multicast Address Range	Multicast addresses are required to transport BUM overlay traffic for the NSX-V hybrid replication mode, which is used by default in Cloud Foundation. Define a set of values that correspond to the NSX Segment ID range.

Application Virtual Networks in Cloud Foundation 3.9.1

Cloud Foundation 3.9.1 uses NSX Data Center for vSphere to create virtual networks, called application virtual networks (AVNs). AVNs use a single IP network address space that spans across datacenters. Starting with Cloud Foundation 3.9.1, vRealize Suite components are deployed to AVNs provided by VXLAN virtual wires, instead of being deployed on a VLAN-backed Distributed Port Group.

Use the deployment parameter sheet to provide the information to create two AVNs; Region A and xRegion. The vRealize Suite components get deployed to these AVNs.

AVN	vRealize Component
Region A	vRealize Log Insight
Region A	vRealize Automation Proxy Agents
xRegion	vRealize Operations Manager
xRegion	vRealize Automation
xRegion	vRealize Suite Lifecycle Manager

Two NSX Edge Services Gateways (ESGs) and a Universal Distributed Logical Router (UDLR) route traffic between the AVNs and the public network. The ESGs handle north-south traffic and the UDLR handles east-west traffic. Routing to the management network and external networks is dynamic and based on the Border Gateway Protocol (BGP).

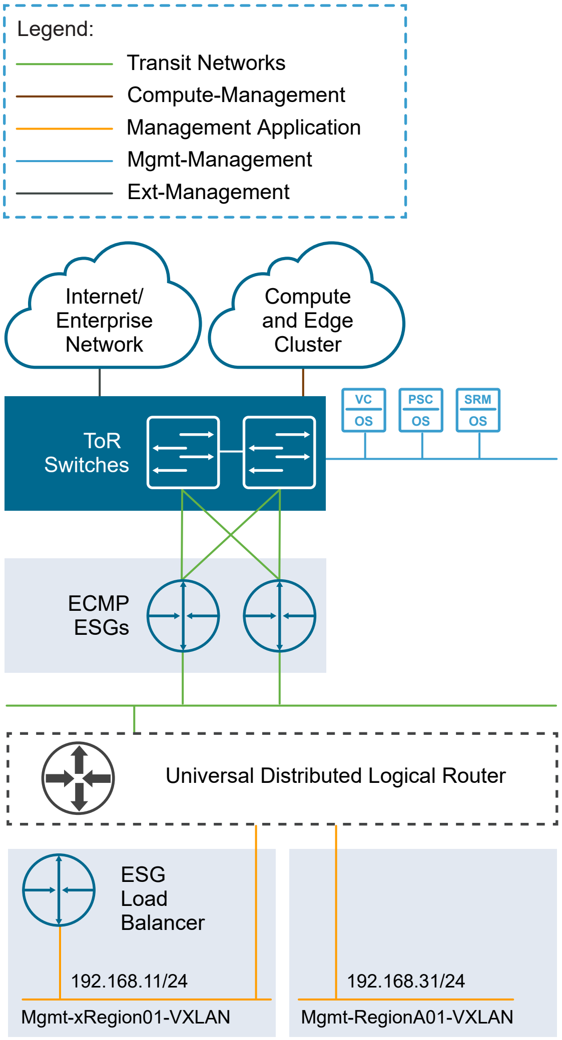


Table 4-18. Edge Services Gateways (ECMP)

Parameter	Value
ESG Name Node 1	Enter a name for the first ESG.
ESG Uplink 1 IP Address Node 1	Enter the first uplink IP address to use Node 1. This is the IP address connected to the first ToR switch.
ESG Uplink 2 IP Address Node 1	Enter the second uplink IP address to use for Node 1. This is the IP address connected to the second ToR switch.
ESG Name Node 2	Enter a name for the second ESG.
ESG Uplink 1 IP Address Node 2	Enter the first uplink IP address to use for Node 2. This is the IP address connected to the first ToR switch.
ESG Uplink 2 IP Address Node 2	Enter the second uplink IP address to use for Node 2. This is the IP address connected to the second ToR switch.

Prepare your top of rack (ToR) switches by configuring Border Gateway Protocol (BGP) on the switches, defining the Autonomous System (AS) number and Router ID, and creating interfaces to connect with Edge Services Gateways (ESGs).

Table 4-19. Top of Rack Switches for BGP Peering

Parameter	Value
Top of Rack 1 - IP Address	Enter the IP address of the first ToR switch.
Top of Rack 1 - BGP Neighbor Password	Enter the BGP neighbor password for the first switch.
Top of Rack 1 - Autonomous System ID	Enter the AS ID for the first switch.
Top of Rack 2 - IP Address	Enter the IP address of the second ToR switch.
Top of Rack 2 - BGP Neighbor Password	Enter the BGP neighbor password for the second switch.
Top of Rack 2 - Autonomous System ID	Enter the AS ID for the second switch. This should match the AS ID for the first switch.

Table 4-20. Application Virtual Networks

Parameter	Value
Region A VXLAN - Logical Switch Name	Enter a name to use for the Region A logical switch.
Region A VXLAN	Enter the gateway IP and CIDR notation to use for the Region A VXLAN.
Region A VXLAN - DNS Search Domain	Enter the DNS search domain for Region A.
Region A VXLAN - DNS Zone	Enter the DNS zone for Region A.
xRegion VXLAN - Logical Switch Name	Enter a name to use for the xRegion logical switch.
xRegion VXLAN	Enter the gateway IP and CIDR notation to use for the xRegion VXLAN.
xRegion VXLAN - DNS Search Domain	Enter the DNS search domain for xRegion.
xRegion VXLAN - DNS Zone	Enter the DNS zone for xRegion.

Table 4-21. NSX-V Licensing Model

Parameter	Value
NSX-V Licensing Model	Choose an option from the drop-down menu, depending on your NSX Data Center for vSphere license. You must have an Enterprise license in order to create a Universal Distributed Logical Router (UDLR). Otherwise, you will created a Distributed Logical Router. With UDLR, you can manually set up a failover region (Region B). DLR does not support this.

Table 4-22. Universal Segment IDs and Multicast Ranges (only with NSX-V Enterprise license)

Parameter	Value
NSX Universal Segment ID Range	Enter the start and end values for the universal segment ID pool. The universal segment ID pool specifies a range for use when building logical network segments. Cross-vCenter NSX deployments use a unique universal segment ID pool to ensure that the universal logical switches VXLAN network identifiers (VNIs) are consistent across all secondary NSX Managers. When determining the size of each segment ID pool, keep in mind that the segment ID range controls the number of logical switches that can be created. If VXLAN is in place in another NSX deployment, consider which VNIs are already in use and avoid overlapping VNIs. Non-overlapping VNIs is automatically enforced within a single NSX Manager and vCenter environment. Local VNI ranges can't be overlapping. However, it's important for you make sure that VNIs do not overlap in your separate NSX deployments. Non-overlapping VNIs is useful for tracking purposes and helps to ensure that your deployments are ready for a cross-vCenter environment.
NSX Universal Multicast Address Range	Enter the start and end values for the universal multicast address range. You must ensure that the multicast address range specified does not conflict with other multicast addresses assigned on any NSX Manager in a cross-vCenter NSX environment. Do not use 239.0.0.0/24 or 239.128.0.0/24 as the multicast address range, because these networks are used for local subnet control, meaning that the physical switches flood all traffic that uses these addresses. For more information about unusable multicast addresses, see https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01.

Table 4-23. (Universal) Distributed Logical Router

Parameter	Value
(Universal) Distributed Logical Router - MTU Size	Depending on your NSX-V license, enter the MTU for the UDLR or DLR. The minimum MTU is 1600 and the recommended MTU is 9000. The value entered here must match the MTU of the physical network.
UDLR/DLR Node Name	Enter name to use for the UDLR/DLR.
UDLR/DLR ESG Autonomous System (AS) ID	Enter an AS ID to use for the UDLR/DLR. This should be different from the AS ID for the ToR switches.
UDLR/DLR ESG BGP Neighbor Password	Enter a BGP neighbor password to use for the UDLR/DLR.
UDLR/DLR ESG Node 1 IP Address	Enter an IP address from the pool of IP addresses reserved for the UDLR/DLR subnet to assign to the uplink interface connecting the UDLR/DLR to ESG node 1.

Table 4-23. (Universal) Distributed Logical Router (continued)

Parameter	Value
UDLR/DLR ESG Node 2 IP Address	Enter an IP address from the pool of IP addresses reserved for the UDLR/DLR subnet to assign to the uplink interface connecting the UDLR/DLR to ESG node 2.
UDLR/DLR ESG Forwarding IP	The forwarding address is the IP address that you assign to the distributed logical router's interface facing its BGP neighbor (its uplink interface). Enter an IP address from the pool of IP addresses reserved for the UDLR/DLR subnet.
UDLR/DLR ESG Protocol IP	The protocol address is the IP address that the logical router uses to form a BGP neighbor relationship. It can be any IP address in the same subnet as the forwarding address, but this IP address must not be used anywhere else. Enter an IP address from the pool of IP addresses reserved for the UDLR/DLR subnet. When youCloud Foundation configures BGP peering between an edge services gateway (ESG) and a logical router, it uses the protocol IP address of the logical router as the BGP neighbor IP address of the ESG.
UDLR/DLR Network CIDR Notation	Reserve an unused /24 subnet for UDLR/DLR configuration. Enter the CIDR notation for the UDLR/DLR network.

Deploy Parameters Tab: vRealize Log Insight

Enter host names and IP addresses for vRealize Log Insight load balancer and the three physical nodes.

The specified host names and IP addresses must be resolvable using the DNS servers provided earlier, both forward (hostname to IP) and reverse (IP to hostname), otherwise the bring-up process will fail.

The requirements vary depending on your version of Cloud Foundation.

For Cloud Foundation 3.9, each IP address must be part of the management VLAN. This is the same VLAN and IP address space where the vCenter, Platform Services Controller, and ESXi Management VMkernels reside.

For Cloud Foundation 3.9.1, each IP address must be part of the Region A VXLAN. See Application Virtual Networks in Cloud Foundation 3.9.1.

Table 4-24. vRealize Log Insight Servers

Parameter	Value
vRealize Log Insight Load Balancer	Enter host name and IP address of vRealize Log Insight load balancer.
vRealize Log Insight Node #1 (Master)	Enter host name and IP address of vRealize Log Insight master node.
vRealize Log Insight Node #2 (Worker)	Enter host name and IP address of the vRealize Log Insight worker node.

Table 4-24. vRealize Log Insight Servers (continued)

Parameter	Value
vRealize Log Insight Node #3 (Worker)	Enter host name and IP address of the vRealize Log Insight worker node.
vRealize Log Insight Node Size (Default Medium)	Select the initial size of Log Insight appliances. Default size is medium.

Deploy Parameters Tab: SDDC Manager

Enter the host name, IP address, and subnet mask of the SDDC Manager VM.

Table 4-25. SDDC Manager

Parameter	Value
SDDC Manager Host name	Enter a host name for the SDDC Manager VM. The specified host name must be registered with your DNS server for both forward and reverse resolution, and it must be resolvable from the Cloud Foundation Builder VM.
SDDC Manager IP Address	Enter an IP address for the SDDC Manager VM. The IP address must be registered with your DNS server for both forward and reverse resolution, and must be part of the management VLAN.
SDDC Manager Subnet Mask	Enter the subnet mask for the SDDC Manager VM.
Host Pool Name	Enter the network pool name for the management domain network pool.

Upload the Deployment Parameter Spreadsheet and Complete Deployment

You upload the completed deployment parameter spreadsheet to complete bring-up.

Procedure

1 Upload the deployment parameter sheet in one of the following ways. In the Download Spreadsheet section, click **Next**.

- For Cloud Foundation 3.9, click **Upload**, select the completed parameter sheet, and click **Open**.
- For Cloud Foundation 3.9.1, follow the steps below. .

  a In the Download Spreadsheet section, click **Next**.

  b In the Complete Spreadsheet section, click **Next**.

  c In the Upload Spreadsheet section, click **Select File**. Select the completed parameter sheet and click **Open**.

2 After the file is uploaded, click **Next** to begin validation of the uploaded file. You can download or print the validation list.

The following audit tasks are performed and validation results are displayed on the UI.

Task	Validation
JSON validation	Validates JSON correctness, syntax, null values, and missing fields or components
Host and IP DNS records	Validates forward and reverse lookup for all hosts in bring-up JSON.
ESXi Host Readiness	Validates SSH access and policy, NTP configuration and policy, DNS configuration, VMNIC availability, vSwitch availability, VM network portgroup , and VLAN check on each host.
vSAN Disk Availability	Validates that required disks for VSAN are available for use.
License Key Format	Validates format, validity, and expiry for ESX, VSAN, vCenter Server, NSX, and Log Insight license keys.
Password Validation	Validates specified passwords. Checks for minimum length, invalid characters, and format.
Network Configuration	Validates CIDR to IP address validity, IP addresses in use, gateways, invalid or missing VLANs, invalid or missing MTU, IP pools, and network spec availability for all components.
Network Connectivity	Validates that the vSAN and vMotion VLANs, MTUs, and gateways specified in the parameter sheet are correctly configured.
Time Synchronization	Validates NTP configuration for all ESX hosts.
Network IP Pools	Validates the following: ■ Pool defines enough IP addresses such that there is one IP address available for each host used for bring-up. ■ Start and end of IP inclusion pools are within the subnet specified for vSAN and vMotion. ■ IP addresses provided in inclusion pool are not in use.
Cloud Builder Readiness	Validates that Cloud Builder has the correct NTP and DNS configuration.
ESXi Host Version	Validates ESXi version installed on the hosts and compares against the VCF-EMS manifest located in `/opt/evosddc/bundle/scripts/manifest.json` on the Cloud Foundation Builder VM

To access the bring-up log file, SSH to the Cloud Builder VM as root and open the `/opt/vmware/bringup/logs/vcf-bringup-debug.log` file.

If there is an error during the validation and the Next button is grayed out, you can either make corrections to the environment or edit the JSON file and upload it again. Then click **Re-Try** to perform the validation again.

If any warnings are displayed and you want to proceed, click **Acknowledge** and then click **Next**.

3 Click **Deploy SDDC**.

During the bring-up process, the following tasks are completed.

- PSC, vCenter Server, vSAN, vRealize Log Insight, and NSX components are deployed.
- The management domain is created, which contains the management components - SDDC Manager, all vCenter Servers, and NSX Managers and Controllers.

The status of the bring-up tasks is displayed in the UI.

After bring-up is completed, a green bar is displayed indicating that bring-up was successful. A link to the SDDC Manager UI is also displayed.

If there are errors during bring-up, see Chapter 5 Troubleshooting Cloud Foundation Deployment for guidance on how to proceed.

4 Click **Download** to download a detailed deployment report. This report includes information on assigned IP addresses and networks that were configured in your environment.

5 After bring-up is completed, click **Finish**.

6 In the SDDC Deployment Completed dialog box, click **Launch SDDC Manager**.

7 Verify the following:

   - View management domain details.
   - Log in to vCenter Server and verify the management cluster, vSAN cluster, and deployed VMs.

8 Power off the Cloud Builder VM.

   The Cloud Builder VM includes the VMware Imaging Appliance, which you can use to install ESXi on additional servers after bring-up is complete. You can delete the Cloud Builder VM to reclaim its resources or keep it available for future server imaging.

   Caution Do not modify or delete any vDS or port groups, or modify the default configuration.

Configure Dual Authentication

You must configure dual authentication in order to perform certain tasks, such as updating or rotating passwords and configuring NSX Manager backups.

You will use the vSphere Client to create a new SSO group (`Sddc_Secured_Access`), add a user to the group, and assign a password to that user. The user is called the privileged user and will be required, along with its password, to perform certain tasks from the SDDC Manager UI or the VMware Cloud Foundation API.

You can create a new SSO user as the privileged user, or use an existing SSO user. If you plan to invoke operations requiring the privileged user as part of an automation solution, you should create a separate SSO user for this purpose. The SSO users used by automation should also be assigned the `No Access` role.

Note The **`administrator@vsphere.local`** user cannot be the privileged user.

Prerequisites

To perform this operation, you need to log in to the management vCenter Server as the `administrator@vsphere.local` user or another user who has the administrator role.

Procedure

1 Log into management vCenter Server using the vSphere Client.

2 Navigate to **Administration > Single Sign On > Users and Groups**.

3 Click the **Users** tab and select the domain from the drop-down list.

4 To create a new user in the selected domain, click **Add User**, enter the required information, and click **Add**.

5 Click the **Groups** tab and click **Add Group**.

6 Create a group named `Sddc_Secured_Access`, add the new or existing user to the group, and click **Add**.

Troubleshooting Cloud Foundation Deployment

5

You can run the SoS tool and review bring-up log files to troubleshoot deployment issues.

This chapter includes the following topics:

SoS Tool Options for Cloud Builder

You can run SoS tool operations in the Cloud Builder VM to debug a failed bring-up of Cloud Foundation.

Note After a successful bring-up, run the SoS tool only through SDDC Manager. See Supportability and Serviceability (SoS) Tool in the *VMware Cloud Foundation Operations and Administration Guide*.

To run the SoS utility in Cloud Builder, SSH in to the Cloud Builder VM using the **admin** administrative account, then enter **su** to switch to the root user, and navigate to the /opt/vmware/sddc-support directory and type ./sos followed by the options required for your desired operation.

```
./sos --option-1 --option-2 ... --option-n
```

SoS Tool Help Options

Use these options to see information about the SoS tool itself.

Option	Description
--help -h	Provides a summary of the available SoS tool options
--version -v	Provides the SoS tool's version number.

SoS Tool Generic Options

These are generic options for the SoS tool.

Option	Description
`--configure-sftp`	Configures SFTP for logs.
`--debug-mode`	Runs the SoS tool in debug mode.
`--force`	Allows SoS operations from theCloud Builder VM after bring-up. **Note** It is recommended that you do not use this option.
`--history`	Displays the last twenty SoS operations performed.
`--log-dir` *LOGDIR*	Specifies the directory to store the logs.
`--log-folder` *LOGFOLDER*	Specifies the name of the log directory.
`--setup-json` *SETUP_JSON*	Custom setup-json file for log collection. SoS prepares the inventory automatically based on the environment where it is running. If you want to collect logs for a pre-defined set of components, you can create a `setup.json` file and pass the file as input to SoS. A sample JSON file is available on the Cloud Builder VM in the `/opt/vmware/sddc-support/` directory.
`--skip-known-host-check`	Skips the specified check for SSL thumbprint for host in the known host.
`--zip`	Creates a zipped tar file for the output.

SoS Tool Options for JSON Generator

Option	Description
`--jsongenerator`	Invokes the JSON generator utility.
`--jsongenerator-input` *JSON_GENERATOR_INPUT*	Specify the input file to be used by the JSON generator utility.
`--jsongenerator-design` *JSON_GENERATOR_DESIGN*	Specify the design file for the SDDC architecture.
`--jsongenerator-supress`	Supress confirmation to force cleanup directory.
`--jsongenerator-logs` *JSONGENERATORLOGS*	Set the directory to be used for logs. Optional.

SoS Tool Options for Platform Audit

Option	Description
`--platformaudit`	Invokes the platform audit operation.
`--platformaudit-dependency`	Executes audit tests with dependencies.
`--platformaudit-input` *FILE*	Specify the input file to be used by the platform audit utility.
`--platformaudit-kill`	Kills all running platform audit processes.
`--platformaudit-modules` *MODULE1,MODULE2,MODULE3*	Specify the specific audit tests to run. If specifying multiple tests, separate the modules with commas.
`--platformaudit-output` *OUTPUT*	Saves the output to the specified file.
`--platformaudit-reason`	Outputs reasons for failed or skipped tests.
`--platformaudit-tree`	Displays a list of available audit tests.

SoS Tool Options for Health Check

These SoS commands are used for checking the health status of various components or services, including connectivity, compute, and storage.

Option	Description
`--certificate-health`	Verifies that the component certificates are valid (within the expiry date).
`--connectivity-health`	Performs a connectivity health check to inspect whether the different components of the system such as the ESXi hosts, Virtual Center Servers, Log Insight VM, NSX Manager VMs, PSC VMs, SDDC Manager VM can be pinged.
`--compute-health`	Performs a compute health check.
`--general-health`	Verifies ESXi entries across all sources, checks the Postgres DB operational status for hosts, checks ESXi for error dumps, and gets NSX Manager and cluster status.
`--get-host-ips`	Returns server information.
`--health-check`	Performs all available health checks.
`--ntp-health`	Verifies whether the time on the components is synchronized with the NTP server in the Cloud Builder VM.
`--services-health`	Performs a services health check to confirm whether services are running
`--run-vsan-checks`	Runs proactive vSAN tests to verify the ability to create VMs within the vSAN disks.

SoS Tool Log File Options

Option	Description
`--api-logs`	Collects output from APIs.
`--cloud-builder-logs`	Collects Cloud Builder logs.
`--dump-only-sddc-java-threads`	Collects only the Java thread information from the SDDC Manager.
`--esx-logs`	Collects logs from the ESXi hosts only. Logs are collected from each ESXi host available in the deployment.
`--no-clean-old-logs`	Use this option to prevent the tool from removing any output from a previous collection run. By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify this option.
`--no-health-check`	Skips the health check executed as part of log collection.
`--nsx-logs`	Collects logs from the NSX Managerand NSX Controller instances only.
`--psc-logs`	Collects logs from the Platform Services Controller instances only.

Option	Description
`--rvc-logs`	Collects logs from the Ruby vSphere Console (RVC) only. RVC is an interface for ESXi and vCenter. **Note** If the Bash shell is not enabled in vCenter, RVC log collection will be skipped . **Note** RVC logs are not collected by default with ./sos log collection.
`--sddc-manager-logs`	Collects logs from the SDDC Manager only.
`--test`	Collects test logs by verifying the files.
`--vc-logs`	Collects logs from the vCenter Server instances only. Logs are collected from each vCenter server available in the deployment.
`--vm-screenshots`	Collects screen shots from all VMs.

Sample Output

The following text is a sample output from an `--ntp-health` operation.

```
root@cloud-builder [ /opt/vmware/sddc-support ]# ./sos --ntp-health --skip-known-host --force
Welcome to Supportability and Serviceability(SoS) utility!

User passed --force flag, Running SOS from Cloud Builder VM, although Bringup is completed
and SDDC Manager is available. Please expect failures with SoS operations.
Health Check : /var/log/vmware/vcf/sddc-support/healthcheck-2018-08-24-10-49-05-7911
Health Check log : /var/log/vmware/vcf/sddc-support/healthcheck-2018-08-24-10-49-05-7911/sos.log
SDDC Manager : sddc-manager.vrack.vsphere.local
NTP : GREEN
+-----+-----------------------------------------+------------+-------+
| SL# |                   Area                  |   Title    | State |
+-----+-----------------------------------------+------------+-------+
|  1  |    ESXi : esxi-1.vrack.vsphere.local    |  ESX Time  | GREEN |
|  2  |    ESXi : esxi-2.vrack.vsphere.local    |  ESX Time  | GREEN |
|  3  |    ESXi : esxi-3.vrack.vsphere.local    |  ESX Time  | GREEN |
|  4  |    ESXi : esxi-4.vrack.vsphere.local    |  ESX Time  | GREEN |
|  5  |     PSC : psc-1.vrack.vsphere.local     | NTP Status | GREEN |
|  6  |     PSC : psc-2.vrack.vsphere.local     | NTP Status | GREEN |
|  7  | vCenter : vcenter-1.vrack.vsphere.local | NTP Status | GREEN |
+-----+-----------------------------------------+------------+-------+

Legend:

 GREEN - No attention required, health status is NORMAL
 YELLOW - May require attention, health status is WARNING
 RED - Requires immediate attention, health status is CRITICAL

Health Check completed successfully for : [NTP-CHECK]
```

The following text is sample output from a `--vm-screenshots` log collection operation.

```
root@cloud-builder [ /opt/vmware/sddc-support ]# ./sos --vm-screenshots
     --skip-known-host --force
```

```
Welcome to Supportability and Serviceability(SoS) utility!

User passed --force flag, Running SOS from Cloud Builder VM, although Bringup is completed
and SDDC Manager is available. Please expect failures with SoS operations.
Logs : /var/log/vmware/vcf/sddc-support/sos-2018-08-24-10-50-20-8013
Log file : /var/log/vmware/vcf/sddc-support/sos-2018-08-24-10-50-20-8013/sos.log
Log Collection completed successfully for : [VMS_SCREENSHOT]
```

Cloud Builder VM Log Files

The Cloud Builder VM contains various log files for different components of the system. The following table describes the important log files that can be used for troubleshooting.

Component	Log Name	Location
JsonGenerator	`jsongenerator-`*timestamp*	`/var/log/vmware/vcf/sddc-support/`
PlatformAudit	`platform-audit-`*timestamp*	`/var/log/vmware/vcf/sddc-support/`
Bringup Service	`vcf-bringup.log`	`/var/log/vmware/vcf/bringup/`
	`vcf-bringup-debug.log`	`/var/log/vmware/vcf/bringup/`
	`rest-api-debug.log`	`/var/log/vmware/vcf/bringup/`
SoS	`sos.log`	`/var/log/vmware/vcf/sddc-support/sos-`*timestamp*`/`

Cloud Foundation Glossary

6

Term	Description
availability zone	Collection of infrastructure components. Each availability zone is isolated from other availability zones to prevent the propagation of failure or outage across the data center.
bring-up	Initial configuration of a newly deployed Cloud Foundation system. During the bring-up process, the management domain is created and the Cloud Foundation software stack is deployed on the management domain.
commission host	Adding a host to Cloud Foundation inventory. The host remains in the free pool until it is assigned to a workload domain.
composability	Ability to dynamically configure servers to meet the needs of your workloads without physically moving any hardware components. You bind disaggregated hardware components (compute, network, storage, and offload components) together to create a logical system based on the needs of your applications.
dirty host	A host that has been removed from a cluster in a workload domain. A dirty host cannot be assigned to another workload domain until it is cleaned up.
decommission host	Remove an unassigned host from the Cloud Foundation inventory. SDDC Manager does not manage decommissioned hosts.
free pool	Hosts in the Cloud Foundation inventory that are not assigned to a workload domain
host	An imaged server.
inventory	Logical and physical entities managed by Cloud Foundation.
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts that contains the management component VMs
network pool	Automatically assigns static IP addresses to vSAN and vMotion vmkernel ports so that you don't need to enter IP addresses manually when creating a VI workload domain or adding a host or cluster to a workload domain.
patch update bundle	Contains bits to update the appropriate Cloud Foundation software components in your management or VI workload domain.
region	A Cloud Foundation instance.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system.
SDDC Manager VM	Virtual machine (VM) that contains the SDDC Manager services and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.

Term	Description
unassigned host	Host in the free pool that does not belong to a workload domain.
workload domain	A policy based resource container with specific availability and performance attributes that combines vSphere, storage (vSAN, NFS, or VMFS on FC) and networking (NSX for vSphere or NSX-T) into a single consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations. It can contain cluster(s) of physical hosts with a corresponding vCenter to manage them. The vCenter for a workload domain physically lives in the management domain.